EMERGING STATE ISSUE

ID THEFT :

- **SECURITY BREACH NOTIFICATION**
- **SECURITY ALERTS**
- **CREDIT FREEZE**
- **VICTIM VERIFICATION PASSPORT**

There is little doubt that identity theft is one of the fastest growing crimes plaguing our Nation. The FTC estimates that in the last 5 years about 27.3 million Americans have been victims of identity theft. Financial losses extend beyond unauthorized credit card charges or loans and cost individuals and financial institutions billions of dollars annually. According to a recent FTC study, the total annual cost of identity theft to its victims is about $5 billion.

Consumers have become powerless to protect themselves from the exposure of their personal data. No amount of individual vigilance can forestall the disclosure of one's Social Security number when it is entrusted to information broker employees who do not properly secure their laptops, or when such personal information is sent unencrypted through the mail.

As a result on this growing national crisis, both federal and state lawmakers have been introducing legislation to provide identity theft victims with tools to help them minimize their losses. Some of the tools include: security breach notification, security alerts, credit report freezes and identity theft victim verification passports.

Security Breach Notification **:** California passed a law in 2002 that required all information brokers to notify consumers of any breach of the security system protecting the consumers' personal information. This law became a national model when in 2004 it was responsible for informing California residents, and drawing the public's attention, to the unauthorized acquisition of 145,000 consumer data profiles at ChoicePoint Inc. (Security breach notification legislation has been passed in : AR, CA, CT, DE, FL, GA. IL, IN, ME, MN, MT, NV, ND,TN, TX, WA)

Security Alerts : This is a statement added to a consumer's credit report and credit score asking issuers to check with the consumer prior to issuing credit. This provision was included in the 2003 Fair and Accurate Credit Transaction Act (FACT Act).

Credit Freeze : This allows consumers to "freeze" their credit reports so that when a credit reporting agency receives a request for the consumer's credit report the requester will be told that the report is unavailable for viewing. (Credit freeze legislation has been passed in : CO, CT, IL, LA, ME, NJ, NV, TX, VT, WA)

Victim Verification Passport : This allows ID theft victims who have filed police reports to apply to a state law enforcement agency for an ID Theft Verification Card. The victim's information is entered into a statewide database and shared among state agencies to assist in the apprehension of the thief. The Verification Card is used by the victim to prove fraudulent transactions to creditors, as well as to protect the victim from unnecessary detention and arrest for crimes committed by the thief.

THE CREDIT FREEZE DEBATE

Recent data leaks of personal information have resulted in over 1 million notification letters being sent to consumers telling them they may be vulnerable to identity theft. But the question is then, "What do I do now?" A current debate is underway in several state legislatures as to whether a security alert is enough, or whether victims should be allowed to voluntarily freeze their credit reports to stop ID thieves from accessing the reports to obtain fraudulent credit :

Combating Identity Theft VS. Limiting Access to Instant Credit

Credit Freeze Proponents : A credit freeze is the most effective tool to combat identity theft. It is a proactive tool that will allow people to stop an identity theft before it occurs.

Credit Freeze Opponents : A credit freeze is an extreme step that is not necessary because federal law now allows for security alerts. The new security alert requirements should be given time to take effect.

Credit Freeze Proponents : Some reports have indicated that security alerts are ineffective because creditors are not required to honor them. It is argued that they are often ignored by creditors who are willing, for example, to gamble that the potential plasma TV purchaser is legitimate, and write off any losses that might occur if the person turns out to be a fraud.

Credit Freeze Opponents: A credit freeze will slow down a consumer's lending process by several days, so it is not a good idea for people who apply for credit or change jobs frequently.

Credit Freeze Proponents : Although it will slow down one's credit, it will not stop it. Credit freezes are voluntary. For some consumers, the choice of using a credit freeze would be a trade-off between potential identity theft and inconvenience.

Credit freezes, generally, do not apply to entities that have an existing account with the consumer, nor to selected users that a consumer has indicated should be exempt from the freeze. Credit freezes can be "thawed" upon request by the consumer for a specific user or a specified period of time.

Credit Freeze Opponents : Thawing a credit freeze requires an easily forgotten, rarely used PIN, and can take several days. This could be a problem if a consumer looses a cell phone and needs to replace it quickly, or wants to receive a 10% discount through retail credit at point of purchase.

OTHER ISSUES TO CONSIDER

Who bears the costs of identity theft?
Federal law limits consumer liability on a credit card to $50 per card, however, when a third party vendor causes the breach, often the issuing financial institution pays the price.

Many financial institutions are playing odds trying to assess the cost of reissuing new cards vs. the cost if their cardholders are victims of actual fraud. The Pennsylvania State Employees Credit Union reissued new cards for 21,300 accounts after two separate security breaches by third party vendors left credit union members vulnerable to identity theft. The credit union also extended its call center hours on weekdays and added Saturday hours to accommodate questions from their members. The costs were well over $100,000, even though the credit union did not cause the breach.

Should the financial institutions that issue the cards be notified, as well as consumers?
Until the financial institutions that issue the compromised credit and debit cards are notified by the third party vendor, they cannot help with fraud prevention, such as canceling and reissuing new cards. In recent cases, the press and public learned of the potential identity theft before the issuing financial institutions.

What type of information should trigger a breach notification?

- Encrypted vs. Unencrypted personal information?
- Names: First and Last; First Initial and Last Name; Last Name only?
- Account numbers, credit / debit card numbers ONLY when linked to security code, access code or PIN?
- Driver's license number?
- Social Security number?

How quickly are consumers notified when a security breach occurs?
Most bills require consumers to be notified in a manner that is as "expedient as possible" or "without unreasonable delay" or "as soon as practicable". Most bills also allow the entity to take necessary measures to determine the scope of the breach and eliminate the leak before having to notify consumers. Additionally, if law enforcement agencies determine that notification could impede an investigation, further delaying the notification may be necessary. In some of the recent cases, identity theft victims were not notified for several months.

How Should a Credit Freeze be Applied?

- Should everyone be allowed to request a credit freeze? Or just persons who have had their personal information breached? Or just those that are actual victims of identity theft?
- Should there be a reasonable fee to request a credit freeze? For everyone? Or just those that are not victims of a security breach?

GUIDELINES FOR STATE LEGISLATION

CUNA's State Credit Union Subcommittee encourages state identity theft legislation that :

- Requires the 3rd party who was exercising control over the consumer's non-public information at the time of the breach to notify financial institutions when a breach has occurred;

- Requires the following information to be included in the financial institution notification:
  - when the breach occurred;
  - Identification of the 3rd party who was exercising control over the consumer's non-public information at the time of the breach;
  - which accounts are affected; and
  - details what type of personal information was compromised;

- Allows financial institutions to disclose the source of the breach to consumers;

- Requires the breaching party to reimburse the consumer or financial institution for any losses and, if security negligence is determined, expenses incurred due to the breach;

CUNA's STATE CREDIT UNION SUBCOMMITTEE

Lee Williams, KS, Chair

Mary Ann Clancy, MA/NH/RI, Vice Chair

Stacy Augustine, WA
Eric D. Estes, NV
John Graham, KY
Fred Healey, MA
Catherine Herring, OH
Dan Kester, CO
Pam Leavitt, OR
Robin H. Marohn, WI
Grace Y. Mayo, CA
Larry D. Nuss, IA
Ron Rioux, NH
Michael Tucker, WV
Jane G. Watkins, VA